安全小课堂第八十九期【web漏洞之逻辑漏洞挖掘】

京东安全应急响应中心 3月26日

逻辑错误漏洞是指由于程序逻辑不严或逻辑太复杂，导致一些逻辑分支不能够正常处理或处理错误，一般出现在任意密码修改（没有旧密码验证）、越权访问、密码找回、交易支付金额。JSRC**安全小课堂第八十九期，**邀请到**Carry_your**作为讲师就**web漏洞之逻辑漏洞挖掘**为大家进行分享。感谢白帽子盆友的精彩提问与互动~

验证码的部分一般哪种逻辑漏洞比较多？

京安小妹

Carry_your:

图片验证码较多的问题是:

a.图片内容比较清晰可识别;

b.验证码采用前端js刷新;

c.验证码不过期;

d.验证码本地校验;

e. 删除数据包中的验证码参数;

短信验证码较多的问题是:

a.验证码4位数字且不过期;

b.验证码未绑定用户;

c.验证码本地校验;

d.验证码编码后存在数据包中（PS一般还能导致短信内容可控）;

e.验证码可复用;

讲师

找回密码的地方一般会有什么逻辑问题?

京安小妹

Carry_your:

a.找回密码的验证码为四位数字可爆破真实验证码;

b.采用本地验证,可以先尝试修改自己的帐号密码，保存正确的返回包，然后修改他人密码的时候替换返回包;

c.最终修改密码的数据包，以另外的ID作为身份判断（例如userid），而该ID在别处可以获取到;

d.接受验证码的手机号修改为自己的号码，然后输入自己的号码接收到的验证码去进行密码重置;

e.获取验证码的时候，会生成一个身份标识（例如cookie值），那么我们就替换他人账号的身份证重置他人的密码;

还有一些其他的方法这里就不一一描述了，可以去i春秋看我之前发过的一篇专门针对密码重置的视频。

视频地址:

https://www.ichunqiu.com/course/59045

讲师

在线购买商品的时候，除了修改金额还有没有别的逻辑漏洞?

京安小妹

Carry_your:

a.添加两个商品，其中一个商品的数量为负数，在总价上抵消另外一个商品的价格，造成总价格为100*1+99*-1的结果，最终以1元支付；

b.使用例如满200元-100元的优惠券，然后在交易过程中替换商品价格为101元的商品id，最终以1元支付；

c.支付结果判断采用本地验证，通过修改返回包让系统误以为我们已成功支付，从而商品状态变为已支付状态；

d.限量购买的商品，比如没人限购1件，如果缺少数据加锁机制，择可以通过数据包并发的方式来突破限制；

e.购买商品未支付的时候，商品库存值已经扣掉相应数量，且订单未设置自动取消时间，批量操作即可导致商城所有商品无法购买；

f.越权使用他人余额来给我们支付商品，付款的时候修改数据包中的用户ID即可，有些需要支付密码的，我们可以通过暴力破解的方式进行测试。注意这里一般是使用一个简单的密码如123456，然后对用户ID进行遍历会比较容易成功；

g.商品下单的时候，一般通过修改数据暴力的地址id，然后去查看订单的时候就可以获取他人的地址等信息。

后台管理系统中，如果你有一个普通帐号，如何尝试获取管理员权限?

京安小妹

Carry_your：

a.编辑个人信息的时候，修改权限组的id，一般管理员的值为0或者1；

b.后台修改密码的地方，如果是根据userid来修改密码的，可以修改id的值来修改管理员的密码；

c.在个人资料处插入XSS脚本，一般能打到管理员cookie的概率很大；

d.查看个人资料的时候，如果是根据id来显示，一般都有越权，可以遍历id获取管理员信息；

e.测试后台功能，找一下注入、上传、命令执行等漏洞，直接拿下数据库权限或者shell，再找管理员权限就轻而易举了。

讲师

显示个人用户信息的地方可能会出现什么问题？

京安小妹

Carry_your:
XSS、越权、信息泄漏、文件上传、sql注入;
a.XSS的话，一般只能打到自己或者管理员，而只有后者有用;
b.越权的话一般是越权查看和编辑他人的个人信息，有时候我们还可以通过在数据包里添加一些参数来做到修改系统不允许修改的信息，如手机号、用户名等;
c.信息泄漏一般是后台执行了select *，导致用户的所有信息都在返回包里，包括该用户的密码、密保答案等不应该返回的信息;
d.头像处的文件上传，一般是任意文件上传漏洞、ImageMagick命令执行等，有时候也会存在XSS和越权的问题;
e.sql注入一般会存在于个人用户信息，选择地区以及上传头像的地方，这里注入出现的比较多;

:
讲师

京东SRC三月境外游活动

正在火热进行中

挖洞即送出境游，参与即有钱+伴手礼!

详情请戳:

如果多9张机票，你会不会跟我一起走?

本期JSRC 安全小课堂到此结束。更多内容请期待下期安全小课堂。如果还有你希望出现在安全小课堂内容暂时未出现，也欢迎留言告诉我们。

安全小课堂的往期内容开通了自助查询，点击菜单栏进入“安全小课堂”即可浏览。

最后，广告时间，京东安全招人，安全开发、运营、风控、安全研究等多个职位虚位以待，招聘内容具体信息请扫描二维码了解。

简历请发送：cv-security@jd.com

微信公众号：jsrc_team

新浪官方微博：京东安全应急响应中心